WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Wednesday, July 05, 2006

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L73	((authenticat$7 near4 drive) and (key adj exchange near2 server) and (key adj exchange near2 client)).clm.	0
☐	L72	(DRIVE and key adj exchange adj server and key adj exchange adj client).clm.	1
☐	L71	(DRIVE and key adj exchange adj server and key adj exchange adj client).clm.	1
☐	L70	725/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	2
☐	L69	709/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	1
☐	L68	726/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	8
☐	L67	360/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	0
☐	L66	386/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	0
☐	L65	713/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	25
☐	L64	380/$.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	14
☐	L63	380/201,277.ccls. and ((content near4 player) and (scambl$7 or encrypt$7) and (authenticat$6 near7 drive$7))	8
☐	L62	(DVD and DRIVE and key adj exchange adj server and key adj exchange adj client).clm.	1
☐	L61	(DVD and DRIVE and authenticat$6 and key adj exchange adj server and key adj exchange adj client).clm.	0
☐	L60	(386/1).ccls. and (authenticat$7 and drive$3)	3
☐	L59	(386/1).ccls. and (authenticat$7 same drive$3)	1
☐	L58	(360/1).ccls. and (content adj scrambl$8)	0
☐	L57	(360/1).ccls. and (authenticat$7 same content adj scrambl$8)	0
☐	L56	(360/1).ccls. and (authenticat$7 same Drive$7)	0
☐	L55	(725/25).ccls. and (DVD adj drive)	14
☐	L54	(725/25).ccls. and (DVD adj drive same encrypt$8$7)	1
☐	L53	(725/25).ccls. and (DVD adj drive same scrambl$7)	1
☐	L52	L51 and (content same DVD same drive)	2
☐	L51	(713/171 |713/380).ccls.	586

☐	L50	DVD adj changer$2 and key	22
☐	L49	DVD adj changer$2 same key	4
☐	L48	DVD adj changer$2 and key adj exchange	1
☐	L47	changer and key adj exchange	14
☐	L46	DVD adj changer and key adj exchange	1
☐	L45	jukebox and key adj exchange	24
☐	L44	jukebox same key adj exchange	0
☐	L43	DVD adj jukebox and (encrypt$7 same key)	4
☐	L42	DVD adj jukebox same encrypt$7	3
☐	L41	L38 and home adj network	11
☐	L40	L38 same home adj network	0
☐	L39	L38 same homenetwork	0
☐	L38	DVD adj drive same encrypt$7	120
☐	L37	DVD adj changer and encrypt$7	9
☐	L36	DVD adj changer same encrypt$7	4
☐	L35	L32 same key same encrypt$7	1
☐	L34	L32 and copy adj protection	3
☐	L33	L32 same copy adj protection	0
☐	L32	jukebox near3 server	151
☐	L31	jukebox near3 server and hoem adj network	0
☐	L30	jukebox near3 server same hoem adj network	0
☐	L29	jukebox adj server same hoem adj network	0
☐	L28	jukebos adj server same hoem adj network	0
☐	L27	6,055,314.pn.	2
☐	L26	home adj network same (DVD same key)	20
☐	L25	L23 same key	9
☐	L24	L23 near4 key	1
☐	L23	jukebox near4 server	192
☐	L22	server near4 DVD adj changer and key	1
☐	L21	server near4 DVD adj changer and key	1
☐	L20	server near4 DVD adj changer	4
☐	L19	L18 and encrypt$7	4
☐	L18	(DVD near2 changer$3) and (key)	49
☐	L17	(DVD near2 changer$3) and (encryption same key)	1
☐	L16	(DVD near2 changer same key)	8
☐	L15	DVD near2 changer near3 key	2
☐	L14	pass$6 near4 key near3 DVD	7

☐	L13	DVD adj drive near10 client near10 server	17
☐	L12	6,546,193.pn.	4
☐	L11	((key near2 exchange) and (authenticat$7 near6 drive)and (key near2 exchange near2 client) and (key near2 exchange near2 server)).clm.	0
☐	L10	(chan or maymoudes or microsoft) and CSS and (key near2 exchange) and (authenticat$7 near6 drive)	4
☐	L9	(chan or maymoudes or microsoft) and CSS and (key near2 exchange) and (authenticat$7 nea6 drive)	20
☐	L8	(chan or maymoudes or microsoft) and CSS and (key near2 exchange)	20
	DB=DWPI; PLUR=YES; OP=OR		
☐	L7	(chan or maymoudes or microsoft) and CSS and (key near2 exchange)	0
☐	L6	(chan or maymoudes) and CSS	0
☐	L5	content near6 player and scrambl$7	7
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L4	content near6 player and scrambl$7	515
	DB=DWPI; PLUR=YES; OP=OR		
☐	L3	content near6 player and scrambl$7 and CSS	0
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR		
☐	L2	content near6 player same scrambl$7 and CSS	27
☐	L1	secure near4 content near6 player same scrambl$7	8

END OF SEARCH HISTORY

Terms used **secure content player authenticating drive** Found **8,235** of **178,880**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Digital rights management for content distribution
Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard
January 2003 **Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21 CRPITS '03**
Publisher: Australian Computer Society, Inc.
Full text available: pdf(224.63 KB) Additional Information: full citation, abstract, references, citings, index terms

Transferring the traditional business model for selling digital goods linked to physical media to the online world leads to the need for a system to protect digital intellectual property. Digital Rights Management(DRM) is a system to protect high-value digital assets and control the distribution and usage of those digital assets. This paper presents a review of the current state of DRM, focusing on security technologies, underlying legal implications and main obstacles to DRM deployment with the ...

Keywords: DRM, digital content

2 Session 7: content watermarking: Multimedia content screening using a dual watermarking and fingerprinting system
Darko Kirovski, Henrique Malvar, Yacov Yacobi
December 2002 **Proceedings of the tenth ACM international conference on Multimedia**
Publisher: ACM Press
Full text available: pdf(262.42 KB) Additional Information: full citation, abstract, references, citings

We present a new dual watermarking and fingerprinting system, where initially all copies of a protected object are identically watermarked using a secret key, but individual detection keys are distinct. By knowing a detection key, an adversary cannot recreate the original content from the watermarked content. However, knowledge of any one detection key is sufficient for modifying the object so that a detector using that key would fail to detect the marks. Detectors using other detection keys wou ...

3 DRM experience: Digital rights management in a 3G mobile phone and beyond
Thomas S. Messerges, Ezzat A. Dabbish
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: Additional Information: full citation, abstract, references, citings, index

pdf(306.59 KB) terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

4 Invited Talks: Secure information sharing enabled by Trusted Computing and PEI models

Ravi Sandhu, Kumar Ranganathan, Xinwen Zhang

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM Press

Full text available: pdf(210.37 KB) Additional Information: full citation, abstract, references, index terms

The central goal of secure information sharing is to "share but protect" where the motivation to "protect" is to safeguard the sensitive content from unauthorized disclosure (in contrast to protecting the content to avoid loss of revenue as in retail Digital Rights Management). This elusive goal has been a major driver for information security for over three decades. Recently, the need for secure information sharing has dramatically increased with the explosion of the Internet and the convergenc ...

Keywords: PEI models, access control, authorization, secure information sharing, security framework, trusted computing

5 Marking and tracing methods: Traitor tracing for prerecorded and recordable media

Hongxia Jin, Jeffery Lotspiech, Stefan Nusser

October 2004 **Proceedings of the 4th ACM workshop on Digital rights management**

Publisher: ACM Press

Full text available: pdf(188.04 KB) Additional Information: full citation, abstract, references, index terms

In this paper we are focusing on the use of a traitor tracing scheme for distribution models that are based on prerecorded or recordable physical media. When a pirated copy of the protected content is observed, the traitor tracing scheme allows the identification of at least one of the real subscribers who participated in the construction of the pirated copy. We show how we systematically assign the variations to users. We explore under what circumstances traitor tracing technology is applica ...

Keywords: content protection, security, traitor tracing

6 Reception and posters: Securing media for adaptive streaming

Chitra Venkatramani, Peter Westerink, Olivier Verscheure, Pascal Frossard

November 2003 **Proceedings of the eleventh ACM international conference on Multimedia**

Publisher: ACM Press

Full text available: pdf(233.56 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper describes the ARMS system which enables secure and adaptive rich media streaming to a large-scale, heterogeneous client population. The secure streaming algorithms ensure end-to-end security while the content is adapted and streamed via intermediate, potentially untrusted servers. ARMS streaming is completely standards compliant and to our knowledge is the first such end-to-end MPEG-4-based system.

Keywords: MPEG-4, adaptive, encrypted, scalability, streaming, video server

7 Session 6: On perfectly secure communication over arbitrary networks

M V N Ashwin Kumar, Pranava R. Goundan, K Srinathan, C. Pandu Rangan

July 2002 **Proceedings of the twenty-first annual symposium on Principles of distributed computing**

Publisher: ACM Press

Full text available: pdf(965.45 KB) Additional Information: full citation, abstract, references

We study the interplay of network connectivity and perfectly secure message transmission under the corrupting influence of generalized Byzantine adversaries. It is known that in the threshold adversary model, where the Byzantine adversary can corrupt upto any t among the n players (nodes), perfectly secure communication among any pair of players is possible if and only if the underlying synchronous network is $(2t + 1)$-connected. Strictly generalizing these results to the non ...

Keywords: adversary structures, information-theoretic security, secure communication, secure multiparty computation

8 Virtual machine monitors: Terra: a virtual machine-based platform for trusted computing

Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh

October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**

Publisher: ACM Press

Full text available: pdf(140.31 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

9 E-government services and policy track: A secure and private clarke tax voting protocol without trusted authorities

Changjie Wang, Ho-fung Leung

March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**

Publisher: ACM Press

Full text available: pdf(323.54 KB) Additional Information: full citation, abstract, references, index terms

Electronic voting has become one of the most popular activities over the Internet. Security and privacy are always regarded as crucial factors in electronic voting system

design. Various secure voting schemes have been proposed in the past several years to ensure the safe operation of electronic voting and most of them have focused on the common *"one man, one vote"* plurality voting. In this paper, we study on the security and privacy issues in the Clarke tax voting protocol, another impor ...

Keywords: Clarke tax voting protocol, ElGamal encryption, electronic voting, mix network, privacy protection, security, universal verification

10 Q focus: mobile applications: Mobile media: making it a reality

Fred Kitson
May 2005 **Queue**, Volume 3 Issue 4
Publisher: ACM Press
Full text available: pdf(528.08 KB) html(31.52 KB) Additional Information: full citation, abstract, references, index terms

Two prototype apps reveal the challenges in delivering mobile media services.

11 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste
August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**
Publisher: ACM Press
Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

12 Demonstration session 1: ARMS: adaptive rich media secure streaming

Lisa Amini, Raymond Rose, Chitra Venkatramani, Olivier Verscheure, Peter Westerink, Pascal Frossard
November 2003 **Proceedings of the eleventh ACM international conference on Multimedia**
Publisher: ACM Press
Full text available: pdf(179.94 KB) Additional Information: full citation, abstract, references, index terms

In this demonstration we present the ARMS system which enables secure and adaptive rich media streaming to a large-scale, heterogeneous client population. The ARMS system dynamically adapts streams to available bandwidth, client capabilities, packet loss, and administratively imposed policies - all while maintaining full content security. The ARMS system is completely standards compliant and to our knowledge is the first such end-to-end MPEG-4-based system.

Keywords: MPEG-4, adaptive, encrypted, scalability, streaming, video server

13 Processor microarchitecture II: AEGIS: architecture for tamper-evident and tamper-resistant processing

G. Edward Suh, Dwaine Clarke, Blaise Gassend, Marten van Dijk, Srinivas Devadas
June 2003 **Proceedings of the 17th annual international conference on Supercomputing**
Publisher: ACM Press
Full text available: pdf(286.90 KB) Additional Information: full citation, abstract, references, citings, index terms

We describe the architecture for a single-chip aegis processor which can be used to build computing systems secure against both physical and software attacks. Our architecture assumes that all components external to the processor, such as memory, are untrusted. We show two different implementations. In the first case, the core functionality of the operating system is trusted and implemented in a security kernel. We also describe a variant implementation assuming an untrusted operating s ...

Keywords: certified execution, secure processors, software licensing

14 Systems: Towards multilateral secure digital rights distribution infrastructures
André Adelsbach, Markus Rohe, Ahmad-Reza Sadeghi
November 2005 **Proceedings of the 5th ACM workshop on Digital rights management DRM '05**
Publisher: ACM Press
Full text available: pdf(332.27 KB) Additional Information: full citation, abstract, references, index terms

Digital Rights Management (DRM) systems and applications appear to increasingly attract the interest of e-commerce business developers. DRM systems aim at secure distribution of digital content and commonly comprise a huge variety of different technologies. Current DRM systems focus mainly on right-holder's security needs and commonly neglect those of consumers. In particular, these systems even lack reliable means for users to verify that they purchase usage-rights on works (licenses) from the ...

Keywords: DRM, authorship, copyrights, digital distribution chains, licensing and transfer of rights, right ownership, usage rights

15 The IP war: apocalypse or revolution?
Tsvi Gal, Howard M. Singer, Laird Popkin
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**
Publisher: ACM Press
Full text available: pdf(248.96 KB) Additional Information: full citation, abstract, references, index terms

In the Foundation series, Asimov predicted a 1,000 years of darkness following the fall of the galactic empire. In the book Noir, K.W Jeter describes a world where IP is the ultimate war. Combine them together and you have likely scenario No. 1.The Internet era enabled communication and information exchange on a global scale. But it also opened the door to copyright infringement on a global scale. Music, books, movies, software, games, speeches, research papers - everything is now fair game. The ...

Keywords: digital distribution, digital rights management, intellectual property, on-line music

16 DRM experience: Analysis of security vulnerabilities in the movie production and distribution process
Simon Byers, Lorrie Cranor, Dave Korman, Patrick McDaniel, Eric Cronin
October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management**

DRM '03
Publisher: ACM Press

Full text available: pdf(285.80 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Unauthorized copying of movies is a major concern for the motion picture industry. While unauthorized copies of movies have been distributed via portable physical media for some time, low-cost, high-bandwidth Internet connections and peer-to-peer file sharing networks provide highly efficient distribution media. Many movies are showing up on file sharing networks shortly after, and in some cases prior to, theatrical release. It has been argued that the availability of unauthorized copies directl ...

Keywords: digital rights management, file sharing, insider attacks, multimedia, physical security, policy

17 A secure multicast protocol with copyright protection

Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain
April 2002 **ACM SIGCOMM Computer Communication Review**, Volume 32 Issue 2
Publisher: ACM Press

Full text available: pdf(301.97 KB) Additional Information: full citation, abstract, references, citings, index terms

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

Keywords: copyright protection, key distribution, multicast security, watermark

18 Game theory: Completely fair SFE and coalition-safe cheap talk

Matt Lepinski, Silvio Micali, Chris Peikert, Abhi Shelat
July 2004 **Proceedings of the twenty-third annual ACM symposium on Principles of distributed computing**
Publisher: ACM Press

Full text available: pdf(248.65 KB) Additional Information: full citation, abstract, references, index terms

Secure function evaluation (SFE) enables a group of players, by themselves, to evaluate a function on private inputs as securely as if a trusted third party had done it for them. A *completely fair* SFE is a protocol in which, conceptually, the function values are learned *atomically*.We provide a completely fair SFE protocol which is secure for *any number* of malicious players, using a novel combination of computational and physical channel assumptions.We also show how co ...

Keywords: correlated equilibrium, game theory, mechanism design, secure function evaluation

19 Session 8A: Non-interactive and reusable non-malleable commitment schemes

Ivan Damgard, Jens Groth
June 2003 **Proceedings of the thirty-fifth annual ACM symposium on Theory of computing**
Publisher: ACM Press

Full text available: pdf(333.10 KB) Additional Information: full citation, abstract, references, citings, index

terms

We consider non-malleable (NM) and universally composable (UC) commitment schemes in the common reference string (CRS) model. We show how to construct non-interactive NM commitments that remain non-malleable even if the adversary has access to an arbitrary number of commitments from honest players - rather than one, as in several previous schemes. We show this is a strictly stronger security notion. Our construction is the first non-interactive scheme achieving this that can be based on the mini ...

Keywords: commitment, non-malleability, one-way function, signature, universal composability

20 Emerging applications: DRM: doesn't really mean digital copyright management

L. Jean Camp

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(258.91 KB) Additional Information: full citation, abstract, references, citings, index terms

Copyright is a legal system embedded in a larger technological system. In order to examine the functions of copyright it is critical to examine the larger technological context of copyright: analog media and printed paper in particular. The copyright system includes both the explicit mechanisms implemented by law and the implicit mechanisms resulting from the technologically determinant features of paper and print. In order to prevent confusion between the legal, technical, and economic elements ...

Keywords: DRM, DeCSS, copyright, design for values, ethics, fair use, intellectual property, science and technology studies

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next